

On the Counting Function of Elliptic Carmichael Numbers

FLORIAN LUCA

Centro de Ciencias Matemáticas,
Universidad Nacional Autónoma de México,
C.P. 58089, Morelia, Michoacán, México
`fluca@matmor.unam.mx`

IGOR E. SHPARLINSKI

Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
`igor@ics.mq.edu.au`

March 8, 2013

Abstract

We give an upper bound for the number elliptic Carmichael numbers $n \leq x$ that have recently been introduced by J. H. Silverman. We also discuss several possible ways for further improvements.

1 Introduction

Let E be an elliptic curve over the field of rational numbers \mathbb{Q} given by an *affine Weierstraß equation*:

$$E : Y^2 = X^3 + aX + b.$$

In particular, it has a nonzero discriminant $\Delta = 4a^3 + 27b^2$. We refer to [7] for a background on elliptic curves.

For a prime p , we define a_p by $\#E(\mathbb{F}_p) = p + 1 - a_p$, where $E(\mathbb{F}_p)$ is the set of \mathbb{F}_p -rational points on the reduction of E modulo p including the point at infinity O_p .

We also recall that if $p \nmid \Delta$, then $E(\mathbb{F}_p)$ has a structure of an Abelian group (see [7, Chapter III, Section 2]).

Since by the *Hasse bound* $a_p = O(p^{1/2})$ (see, for example, [7, Chapter V, Theorem 1.1]), for $\Re s > 3/2$ we can define the L -function

$$L(s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s})^{-1} \prod_{p \mid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

which we expand to the power series

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

(see, for example, [7, Chapter V, Exercise 8.19]).

Slightly relaxing the definition given in [8] and thus expanding the class of numbers we consider, we say that a positive integer n is an *E-Carmichael number* if

- it is not a prime power;
- for any prime divisor $p \mid n$ we have $p \nmid \Delta$;
- for any point $P \in E(\mathbb{F}_p)$ we have

$$(n + 1 - a_n)P = O_p, \tag{1}$$

where both the equation and the group law are considered over \mathbb{F}_p .

Here we show that the sequence E -Carmichael numbers is of asymptotic density zero.

2 Notation

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \leq cV$ holds with some constant $c > 0$. Throughout the paper, any implied constants in the symbols ‘ O ’, ‘ \ll ’ and ‘ \gg ’ may occasionally depend, where obvious, on the curve E , and are absolute otherwise.

We write $\log_1 x = \max\{1, \log x\}$. For an integer $k \geq 2$, we write $\log_k x$ for the iteratively defined function given by $\log_k x = \log_1(\log_{k-1} x)$. When $k = 1$ we omit the subscript and thus understand that all natural logarithms that appear exceed 1.

3 Main Result

For a real $x \geq 1$, let $N_E(x)$ be the number of E -Carmichael numbers $n \leq x$.

Theorem 1. *For a sufficiently large x*

$$N_E(x) \ll x \frac{(\log_3 x)^{1/2} (\log_4 x)^{1/2}}{(\log_2 x)^{1/4}}.$$

4 Preparations

We start with an integer $a \neq 0, \pm 2$ and a special case of a result Serre [6] that gives an upper bound on

$$\pi_E(x; a) = \#\{p \leq x : a_p = a\}.$$

Lemma 2. *The estimate*

$$\pi_E(x; a) \ll \pi(x) \frac{(\log_2 x)^{2/3} (\log_3 x)^{1/3}}{(\log x)^{1/3}}$$

holds for all $a \neq 0, \pm 2$, where the implied constants depend only on the elliptic curve E .

We also need the following result of David and Wu [4, Theorem 2.3 (i)], which improves and generalises several previous bounds (see [2, 3]). For integers a and $b \geq 1$ let

$$\pi_E(x; a, b) = \#\{p \leq x : \#E(\mathbb{F}_p) \equiv a \pmod{b}\}.$$

Let $\varphi(k)$ denote the Euler function of an integer $k \geq 1$.

Lemma 3. *The estimate*

$$\pi_E(x; a, b) \ll \frac{\pi(x)}{\varphi(b)} + x \exp\left(-Ab^{-2}\sqrt{\log x}\right)$$

holds uniformly for $\log x \gg b^{12} \log b$, where the implied constants depend only on the elliptic curve E and A is a positive absolute constant.

5 Proof of Theorem 1

Let t_p be the exponent of the group $E(\mathbb{F}_p)$, that is, the largest possible order of any point $P \in E(\mathbb{F}_p)$.

We see from (1) that for any E -Carmichael number n we have

$$t_p \mid n + 1 - a_n \tag{2}$$

for all primes $p \mid n$.

Now fix some $z > y > 1$ and remove $n \leq x$ without a prime divisor in $[y, z]$. Let $\mathcal{E}_1(x)$ be the set of such n . By the Brun sieve, see [9, Section I.4.2] and Mertens' formula, see [9, Section I.1.6], we have

$$\#\mathcal{E}_1(x) \ll x \prod_{y \leq p \leq z} \left(1 - \frac{1}{p}\right) = O\left(x \frac{\log y}{\log z}\right). \tag{3}$$

Then remove all $n \leq x$ such that $p^2 \mid n$ for some $p \geq y$. Let $\mathcal{E}_2(x)$ be the set of such n . Fixing p , the number of $n \leq x$ which are divisible by p^2 is at most x/p^2 . Hence,

$$\#\mathcal{E}_2(x) \leq \sum_{y \leq p \leq z} \frac{x}{p^2} = O\left(\frac{x}{y}\right). \tag{4}$$

Let $P(n)$ be the largest prime factor of n . We remove $n \leq x$ such that $P(n) \leq w$, where

$$w = \exp\left(\frac{\log x \log_4 x}{2 \log_3 x}\right).$$

Put $\mathcal{E}_3(x)$ for the set of such n . It is well-known that

$$\#\mathcal{E}_3(x) = \frac{x}{\exp((1 + o(1))u \log u)},$$

as $x \rightarrow \infty$, where

$$u = \frac{\log x}{\log w} = \frac{2 \log_3 x}{\log_4 x}.$$

Since

$$u \log u = (2 + o(1)) \log_3 x$$

as $x \rightarrow \infty$, we derive

$$\#\mathcal{E}_3(x) = \frac{x}{(\log_2 x)^{2+o(1)}} = O\left(\frac{x}{(\log_2 x)}\right). \quad (5)$$

Assume that $w^{1/2} > 2z$. Then any remaining integer $n \leq x$ can be written under the form $n = pPm$, where $p \in [y, z]$, $P = P(n) > w$ and pP is coprime to m . Since the coefficient a_n is a multiplicative function of n , we have $a_n = a_m a_p a_P$. Then, we see from (2), that

$$t_p | mPp + 1 - a_m a_p a_P. \quad (6)$$

We fix $p \in [y, z]$ count the number of choices for the pair (m, P) . Assume next that $p \mid t_p$. Let $\mathcal{E}_4(x)$ be the number of such n . In this case, $t_p = p$, $a_p = 1$ and congruence (6) shows that $p \mid a_m P$.

Estimating the number of such products $mP \leq x/p$ trivially as $O(x/p)$, summing up over all $p \in [y, z]$ with $a_p = 1$ and using Abel's summation formula and Lemma 2, we derive

$$\#\mathcal{E}_4(x) \ll \sum_{\substack{y \leq p \leq z \\ a_p = 1}} \frac{x}{p} \ll \frac{x(\log_2 y)^{2/3}(\log_3 y)^{1/3}}{(\log y)^{1/3}}. \quad (7)$$

From now on, we assume that t_p and p are coprime. Note that $t_p \gg p^{1/2}$ (see [5] for a slightly more precise result). We next write

$$t_p = d_1 d_2,$$

where $d_1 = \gcd(t_p, m)$. Suppose that $d_1 > t_p^{1/2}$ and let $\mathcal{E}_5(x)$ be the set of such $n \leq x$. Then $m = d_1 m_1$, so n is a multiple of $p d_1$. The number of such choices when p and $d_1 \mid t_p$ are fixed is at most $x/pd_1 = O(x/p^{5/4})$. Summing up over all primes p and divisors d_1 of t_p which exceed $t_p^{2/3}$, we get that

$$\#\mathcal{E}_5(x) \ll \sum_{y \leq p \leq z} \frac{\tau(t_p)}{p^{5/4}} = O\left(\frac{x}{y^{1/4+o(1)}}\right) \quad (8)$$

as $y \rightarrow \infty$.

Let $\mathcal{E}_6(x)$ be the set of the remaining $n \leq x$. Writing again $m = d_1 m_1$, the divisibility relation (6) implies that $d_1 \mid a_p a_m a_P$. Fix also m and we put $d_3 = \gcd(d_1, a_p)$, $d_4 = \gcd(d_1/d_3, a_m)$, and $d_5 = d_1/(d_3 d_4)$. Then the relation $a_P = d_5 \lambda$ holds with some positive integer λ . Further, the divisibility relation (6) gives

$$d_2 \mid m_1 p P - \left(\frac{a_p}{d_3}\right) \left(\frac{a_m}{d_4}\right) \lambda,$$

and $m_1 p$ is invertible modulo d_2 . This shows that

$$P \equiv \left(\frac{a_p}{d_3}\right) \left(\frac{a_m}{d_5}\right) \lambda \pmod{d_2}. \quad (9)$$

In the right-hand side of the congruence (9), we assume that a_p/d_3 and a_m/d_5 are coprime to d_2 , otherwise $P \mid d_2$, which is impossible since it would lead to

$$w \leq P \leq d_2 \leq t_p < p + 2\sqrt{p} + 1 < 2z,$$

for large x , which is impossible. Observe that the value of $\lambda \pmod{d_2}$ determines both P and a_P modulo d_2 . In turn, these define $\#E(\mathbb{F}_P)$ modulo P . By Lemma 3, we derive that number of such $P \leq x/(mp)$ is of order at most

$$\begin{aligned} & \frac{\pi(x/mp)}{\varphi(d_2)} + \frac{x}{mp} \exp\left(-Ad_2^{-2}\sqrt{\log x}\right) \\ & \ll \frac{x}{mp\varphi(d_2)\log(x/mp)} + x \exp\left(-Ad_2^{-2}\sqrt{\log x}\right), \end{aligned} \quad (10)$$

provided that

$$d_2 \log d_2 \leq (\log(x/mp))^{1/12}.$$

Since $d_2 \leq t_p \leq 2z$ and $x/mp \geq P \geq w$, so

$$\log(x/mp) \geq \log w \geq \frac{\log x \log_3 x}{\log_2 x},$$

it follows that the above inequality holds if we choose

$$z \leq (\log x)^{1/13} \quad (11)$$

and x is sufficiently large. For such values of x and z , the second term in the estimate (10) is

$$x \exp \left(-A d_2^{-2} \sqrt{\log x} \right) \leq x \exp \left(-0.25 A (\log x)^{11/26} \right),$$

and is negligible compared with the first. So, the number of such primes $P \leq x/(mp)$ is of order at most

$$\frac{x}{mp \varphi(d_2) \log(x/mp)} \ll \frac{x \log_2 z}{mp d_2 \log(x/mp)},$$

where we have used that, by the well-known bound on the minimal order of the Euler function (see [9, Section I.5.4]), the lower bound

$$\varphi(d_2) \gg d_2 / \log_2 d_2 \gg d_2 / \log_2 z$$

holds for all $d_2 \leq t_p \leq 2z$. Since $x/(mp) > w/z > w^{1/2}$ and also since $d_2 = t_p/d_1 \geq t_p^{1/2} \gg p^{1/4}$, we get that the above estimate is of order at most

$$\frac{x \log_3 x \log_2 z}{mp d_2 \log x \log_4 x} \ll \frac{x \log_3 x \log_2 z}{mp^{5/4} \log x \log_4 x}.$$

Now we sum up the above inequality over all $p \in [y, z]$, all quadruple of divisors (d_1, d_2, d_3, d_4) of t_p and over all m getting a bound of shape

$$\frac{x \log_3 x \log_2 z}{\log x \log_4 x} \sum_{y \leq p \leq z} \sum_{m \leq x} \frac{\tau(t_p)^4}{mp^{5/4}} \ll \frac{x \log_3 x \log_2 z}{y^{1/4+o(1)} \log_4 x},$$

as $x \rightarrow \infty$. Thus, we get that

$$\#\mathcal{E}_6(x) \leq \frac{x \log_3 x \log_2 z}{y^{1/4+o(1)} \log_4 x} \quad (12)$$

as $x \rightarrow \infty$. From the estimates (3), (4), (5), (7), (8) and (12), we conclude that

$$\begin{aligned} \#N_E(x) \ll x \left(\frac{\log y}{\log z} + \frac{1}{y} + \frac{1}{\log_2 x} + \frac{(\log_2 y)^{2/3} (\log_3 y)^{1/3}}{(\log y)^{1/3}} + \frac{1}{y^{1/4+o(1)}} \right. \\ \left. + \frac{\log_3 x \log_2 z}{y^{1/4+o(1)} \log_4 x} \right). \end{aligned}$$

Since $z \leq (\log x)^{1/13}$, the third term is dominated by the first and the second term is dominated by the fourth. Since $y \leq z \leq (\log x)^{1/13}$, it follows that

$$(\log_2 y)^{2/3}(\log_3 y)^{2/3} \ll (\log_3 x)^{2/3}(\log_4 x)^{2/3},$$

so we see that

$$\frac{(\log_2 y)^{2/3}(\log_3 y)^{1/3}}{(\log y)^{1/3}} + \frac{\log_3 x \log_2 z}{y^{1/4+o(1)} \log_4 x} \ll \frac{(\log_3 x)^{2/3}(\log_4 x)^{2/3}}{(\log y)^{1/3}},$$

provided that

$$y^{1/5} > (\log_3 x)^2 \geq \log_3 x \log_2 z. \quad (13)$$

It now follows easily that

$$\mathcal{N}_E(x) \ll x \left(\frac{\log y}{\log z} + \frac{(\log_3 x)^{2/3}(\log_4 x)^{2/3}}{(\log y)^{1/3}} \right).$$

We now choose

$$z = (\log x)^{1/14} \quad \text{and} \quad y = \exp \left((1/14)(\log_2 x)^{3/4}(\log_3 x)^{1/2}(\log_4 x)^{1/2} \right),$$

thus (11) and (13) are satisfied, and we derive the desired result.

6 Comments

We recall that under the Generalised Riemann Hypothesis, Serre [6] gives a much stronger estimate

$$\pi_E(x; a) \ll \pi(x)x^{-1/6}(\log x)^{2/3}, \quad a \neq 0, \pm 2,$$

instead of that of Lemma 2; we also refer to [1] for a survey of other results and conjectures related to Lemma 2. Furthermore, also under the Generalised Riemann Hypothesis, David and Wu [4, Theorem 2.3 (iii)] show that one has the estimate

$$\pi_E(x; a, b) \ll \frac{\pi(x)}{\varphi(b)}$$

uniformly for $b \ll x^{1/8}/\log x$, instead of that of Lemma 3. Using these bounds in our argument, one can easily obtain a conditional improvement of Theorem 1. It is also possible that for CM curves one can also obtain

stronger results. For example, in [1] one can find a survey of improvements of Lemma 2 for CM curves. There is little doubt that Lemma 3 can also be improved for CM curves. However, in order to get substantially better bounds, our argument, which treats the elements the set $\#\mathcal{E}_1(x)$ trivially and relies on the bound (3), ought to be augmented with some new ideas.

Another approach to a possible improvement of Theorem 1 is via a more efficient treatment of elements of the set $\mathcal{E}_4(x)$. In turn, this leads to a question of obtaining nontrivial upper bounds on the cardinality of the set

$$\{n \leq x : a_n \equiv a \pmod{p}\}$$

for a prime p and an integer a (only the case $a = 1$ is relevant to our applications). Obtaining such bounds is certainly of independent interest.

7 Acknowledgements

The authors would like to thank Alina Cojocaru for useful discussions.

During the preparation of this paper, and F. L. was supported in part by Project PAPIIT IN104512 and a Marcos Moshinsky fellowship and I. S. by ARC Grant DP1092835 (Australia) and by NRF Grant CRP2-2007-03 (Singapore).

References

- [1] A. Cojocaru, ‘Questions about the reductions modulo primes of an elliptic curve’, *Proc. 7th Meeting of the Canadian Number Theory Association (Montreal, 2002)*, CRM Proceedings and Lecture Notes, Vol. 36, Amer. Math. Soc., 2004, 61–79.
- [2] A. Cojocaru, É. Fouvry and M. R. Murty, ‘The square sieve and the Lang–Trotter conjecture’, *Canadian J. Math.* **57** (2005), 1155–1177.
- [3] A. C. Cojocaru, F. Luca and I. E. Shparlinski, ‘Pseudoprime reductions of elliptic curves’, *Math. Proc. Cambridge Philos. Soc.* **146** (2009), 513–522.

- [4] C. David and J. Wu, ‘Pseudoprime reductions of elliptic curves’, *Canadian J. Math.* **64** (2012), 81–101.
- [5] R. Schoof, ‘The exponents of the group of points on the reduction of an elliptic curve’, *Arithmetic Algebraic Geometry*, Progr. Math., vol. 89, Birkhäuser, Boston, MA, 1991, 325–335.
- [6] J.-P. Serre, ‘Quelques applications du théorème de densité de Chebotarev’, *Inst. Hautes Études Sci. Publ. Math.*, **54** (1981), 123–201.
- [7] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.
- [8] J. H. Silverman, ‘Elliptic Carmichael numbers and elliptic Korselt criteria’, *Preprint*, 2011 (available at <http://arxiv.org/abs/1108.3830>).
- [9] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, 1995.